

Appl. No. 09/918,831
Amendment and/or Response
Reply to Office action of 5 May 2005

Page 5 of 8

REMARKS / DISCUSSION OF ISSUES

Claims 1-8 are pending in the application. Claims 9 and 10 are canceled herein.

The applicant thanks the Examiner for the Examiner's thoroughness in assessing the applicant's prior remarks, and for pointing out possible errors in the applicant's interpretation of the prior art. Because the applicant's prior remarks were unpersuasive in affecting the patentability of the claims, the applicant herein retracts any and all prior remarks.

The Office action rejects claims 1-6 under 35 U.S.C. 101. The applicant respectfully traverses this rejection. The Office action asserts that the claims are not tied to a technological art, environment, or machine that would result in a practical application producing a concrete, useful, and tangible result. The applicant notes that generating a linear transformation matrix for use in a symmetric-key cipher is related to the technological art of cryptography, and that the resultant matrix is a concrete, useful, and tangible result.

The Office action rejects:

claims 1, 3-4, and 7-8 under 35 U.S.C. 103(a) over Rijman et al. ("The Cipher SHARK", hereinafter Rijman) and Loureiro et al. ("Function Hiding Based on Error Correcting Codes", hereinafter Loureiro);

claims 2 and 5 under 35 U.S.C. 103(a) over Rijman, Loureiro, and FOLDOC ("brute force"); and

claim 6 under 35 U.S.C. 103(a) over Rijman, Loureiro, Isaka et al. ("Multilevel Coded Modulation...", hereinafter Isaka) and Williams ("Turbo Product Code Tutorial").

The applicant respectfully traverses these rejections.

Appl. No. 09/918,831
Amendment and/or Response
Reply to Office action of 5 May 2005

Page 6 of 8

The applicant respectfully maintains that Rijman and Loureiro address different technologies, and there is no suggestion in either Rijman or Loureiro to combine their teachings. The Office action asserts that the motivation for such a combination would have been "to hide a function represented on a matrix format". The applicant notes that Loureiro teaches hiding a function represented on a matrix format, but neither Rijman nor the applicant's invention addresses hiding a function represented on a matrix format. Thus, this suggestion is only relevant to Loureiro. The fact that Loureiro teaches hiding a function represented on a matrix format does not provide a motivation for combining the teachings of Rijman and Loureiro, and would not lead to the applicant's claimed invention.

However, assuming in argument that Rijman and Loureiro could be combined, the applicant respectfully maintains that neither Rijman nor Loureiro teach or suggest the elements of the applicant's invention.

The Examiner's attention is requested to MPEP 2142, wherein it is stated:

"To establish a *prima facie* case of obviousness ... the prior art reference (or references when combined) *must teach or suggest all the claim limitations*... If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

Claim 1, upon which each of the other claims depend, claims a method of generating a linear transformation matrix A for use in a symmetric-key cipher, that includes generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in \mathbb{Z}_2^{k \times n}$ in a standard form $G = (I_k \parallel B)$, with $B \in \mathbb{Z}_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code; extending matrix B with $2k-n$ columns such that a resulting matrix C is non-singular, and deriving matrix A from matrix C.

The Office action asserts that Rijmen teaches generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in \mathbb{Z}_2^{k \times n}$ in a standard form $G = (I_k \parallel B)$, with $B \in \mathbb{Z}_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code. The applicant respectfully disagrees with this assertion.

Appl. No. 09/918,831
Amendment and/or Response
Reply to Office action of 5 May 2005

Page 7 of 8

Rijmen teaches that a binary $[n,k,d]$ error-correcting code can be represented by a generator matrix $G \in \mathbb{Z}_2^{k \times n}$ in a standard form $G = (I_k \parallel B)$, with $B \in \mathbb{Z}_2^{k \times (n-k)}$, but Rijmen fails to teach the generation of such a code with $k < n < 2k$. Rijmen specifically teaches generating the error-correcting code using $n=2k$, at page 5, to produce a $k \times k$ matrix ($n-k = 2k-k = k$).

The Office action acknowledges that Rijman fails to teach extending matrix B with $2k-n$ columns such that a resulting matrix C is non-singular, and deriving matrix A from matrix C, and the applicant concurs. As the examiner notes, extending the $k \times (k-n)$ matrix B by $2k-n$ columns results in a $k \times k$ matrix C. The applicant notes that there is no suggestion in Rijman to perform such an extension, because Rijman starts with an error correcting code with $n=2k$ to produce a $k \times k$ matrix, and has no need to extend this matrix. In the applicant's claimed invention, the error correcting code is specifically generated with $n < 2k$, and the resultant matrix is expanded to provide a $k \times k$ matrix.

The Office action relies upon Loureiro for teaching extending matrix B with $2k-n$ columns such that a resulting matrix C is non-singular, and deriving matrix A from matrix C, at section 4.1. The applicants respectfully disagrees with this characterization of Loureiro.

At the cited section of Loureiro, Loureiro teaches forming an encrypted function $F' = FGP + E$, where F is a $k \times k$ matrix, G is a $k \times n$ matrix, P is an $n \times n$ matrix, and E is a $k \times n$ matrix. That is, Loureiro teaches expanding a $k \times k$ matrix into a $k \times n$ matrix. Loureiro is silent with regard to an expansion of $2k-n$, as specifically claimed, and is silent with regard to forming a non-singular resulting matrix, as specifically claimed, and is silent with regard to deriving a linear transformation matrix from this non-singular matrix, as specifically claimed.

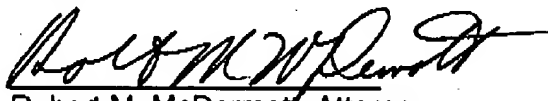
Because neither Rijman nor Loureiro teach or suggest generating a $k \times n-k$ matrix, then expanding it to form a non-singular $k \times k$ matrix, and then deriving a linear transformation matrix from this non-singular matrix, as specifically claimed by the applicant, the applicant respectfully maintains that the rejection of claims 1-8 under 35 U.S.C. 103(a) based on the teachings of Rijman and Loureiro is unfounded.

Appl. No. 09/918,831
Amendment and/or Response
Reply to Office action of 5 May 2005

Page 8 of 8

In view of the foregoing, the applicant respectfully requests that the Examiner withdraw the rejections of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Robert M. McDermott, Attorney
Registration Number 41,508
patents@lawyer.com

1824 Federal Farm Road
Montross, VA 22520
Phone: 804-493-0707
Fax: 215-243-7525